

메타버스 리스크의 국가안보 위협 전망과 시사점

윤정현 부연구위원
yjh5791@inss.re.kr

I. 문제 제기

II. 메타버스 리스크에 대한 국내외 논의 동향

III. 메타버스 공간의 확장·진화에 따른 안보위협 이슈 전망

IV. 시사점과 대응 방안

VISIT...

LANZAROTE
Caliente.COM

국문 초록

코로나19가 촉발한 원격·비대면 트렌드와 함께 최근 온라인 공간과 현실세계가 융합된 디지털 ‘가상 공간세계’로서 ‘메타버스(Metaverse)’가 부상하고 있다. 특히, 메타버스는 현실세계의 대체 공간으로서 사회적 관심을 받으며 일상에서 다양하게 적용되는 중이다. 그러나 이 같은 메타버스 활동 영역의 확장은 사이버 위협에 대한 취약성을 증대시키고 있으며, 가상과 현실의 경계를 초월한 새로운 보안 위협의 발생 가능성도 높이고 있다. 이 같은 메타버스 기반 사이버 위협의 양적·질적 변화에 대해 국가안보 관점에서의 접근 및 제도적 대비는 아직 미비한 상황이다. 이에 본 연구는 메타버스 패러다임이 초래하는 광범위한 국가안보적 위협요소를 전망하고 접근 방향을 제안하고자 하였다. ‘사이버 팬데믹’, ‘딥페이크’, ‘가상자산의 탈취’, ‘테러세력 지원’, ‘디지털트윈 기반 해킹’, ‘민감 정보 프로파일링’ 등 새로운 형태의 메타버스 리스크에 맞서 국가적 차원에서의 시급한 대응이 요구된다. 신종 사이버 위협으로서 메타버스 리스크에 대한 거시적 이해, ‘위협 동기화’에 대비한 거버넌스 체계 수립, 신종 디지털트윈 공격 예방을 위한 ‘능동적 억지’ 전략 수립, 메타버스 데이터·금융거래에 대한 국가의 관리기능 강화가 대표적이라 할 수 있다.

핵심어: 메타버스, 가상융합기술, 사이버팬데믹, 디지털트윈, NFT

목차

- I. 문제 제기
 - II. 메타버스 리스크에 대한 국내외 논의 동향
 - III. 메타버스 공간의 확장·진화에 따른 안보위협 이슈 전망
 - IV. 시사점과 대응 방안
-

I. 문제 제기

1. 팬데믹이 초래한 급속한 디지털화와 사이버 리스크의 대두

- 장기간의 코로나19 확산이 낳은 비대면 패러다임은 사회의 광범위한 디지털 전환과 AI, IoT(사물인터넷), VR·AR(가상·증강현실) 등 융복합 서비스를 확대, 일상의 사이버위협 피해 가능성 증대
 - 정치, 경제, 사회, 문화 등 전 분야에 걸쳐 온라인 활동의 비중이 확대되면서, 일상의 사이버 공간 의존도 역시 급증
 - 비대면 환경에서 경제적 이득을 탈취하기 위한 사이버 범죄조직부터 정치·군사·외교 목적의 국가 배후 조직적 해킹그룹에 이르기까지 사이버 공격의 다양화, 고도화 양상이 관찰되고 있음

2. 메타버스 패러다임의 부상과 사이버 공격 표적 범위의 확대

- 이러한 가운데, 최근 ‘메타버스(metaverse)’¹⁾를 경험하는 이용자가 급증하면서, 사이버공격의 표적 분야 또한 광범위하게 확대 중
 - 메타버스 용어에 대한 학계의 통일된 정의는 부재하나, 초월을 뜻하는 ‘meta’와 우주를 의미하는 ‘universe’가 결합된 합성어로, 다양한 활동가치가 통용될 수 있는 디지털 기반 3차원 가상공간²⁾을 지칭
 - ※ 가상과 현실이 융합된 공간에서 사람·사물이 상호작용하며 경제·사회·문화적 가치를 창출하는 세계로서, 다중의 사용자가 아바타로 상호 소통하고, 현실의 물리적 세계와 동시에 공존할 수 있는 디지털 공간을 의미³⁾

1) 현재 우리정부는 메타버스에 대한 한글 대칭어를 “확장가상세계”로 설명하고 있음.

2) SF작가 닐 스티븐슨(Neal Stephenson)의 소설 ‘Snow Crash(1992)’에 처음으로 등장한 ‘메타버스’는 아바타를 통해 현실과 융합되는 인터넷 기반의 3D 가상세계로 묘사된다. Smart, J.M., Cascio, J. and Paffendorf, J. “Metaverse Roadmap Overview, 2007”. Accelerated Studies Foundation. Retrieved, (2010), pp. 2-3.

3) 김상균·신병호, 『메타버스 새로운 기회 디지털 지구, 경제와 투자의 기준이 바뀐다』, 베가북스, (2021), pp. 4-6.

- 그러나, 디지털 기반 메타버스 활용 영역의 확장은 사이버 위협에 대한 ‘공격표면(Attack Surface)’ 역시 증대시키는 효과를 낳고 있으며, 가상과 현실의 경계를 초월한 새로운 보안 위협도 급증
 - 특히, 사물인터넷(IoT)이 적용된 메타버스 기반 보안 위협 발생 시, 주요 인프라에 대한 물리적 피해와 사회적 혼란 가능성이 제기됨
- “21 사이버위협 분석 및 22 전망 분석”(2021. 12)에 따르면, 메타버스는 AI, NFT와 함께 새로운 유형의 신종 사이버위협⁴⁾의 초래 요소
 - 메타버스 공간 내의 개인정보 및 콘텐츠 침해사고, 가상재화·암호화폐와 관련된 조세 회피, 금융범죄, 현실과 연동된 디지털 트윈 활용 과정에서의 해킹 등 새로운 보안 위협 가능성 등⁴⁾
 - 또한, 메타버스 플랫폼 환경 조작, 인프라 시스템 마비, 통신 네트워크, 데이터의 처리·분석 과정에서 악의적인 해킹 위협이 발생 가능

3. 이 같은 메타버스 기반 사이버 위협의 양적·질적 변화에 대해 국가안보 관점에서의 접근 및 제도적 대비는 아직 미비한 상황

- 메타버스에서 발생할 수 있는 가상과 현실의 융합적 사이버 위협에도 불구하고 현재의 대응체계는 사이버 공간과 물리적 공간을 이분화 하고 있어 법·제도의 정합성 측면에서 문제가 제기됨
 - 또한, 현재와 같은 파편적인 거버넌스 구조로는 거시적인 메타버스 안보 위협에 대한 지원과 대응이 어려운 한계를 내재
- 따라서, 본 연구는 메타버스 패러다임이 초래할 수 있는 광범위한 국가안보적 위협요소에 대해 전망하고 이에 부합하는 새로운 접근 방향에 대해 제안하고자 함

4) 과학기술정보통신부, “21년 사이버위협 분석 및 22년 전망 분석”, (2021.12.24.), p. 4.

II. 메타버스 리스크에 대한 국내외 논의 동향

1. 세계경제포럼(WEF)에서 제기된 메타버스 안전이슈

- 물리적 세계와 가상세계의 경계가 모호해지면서 새롭게 제기될 수 있는 잠재적 위험이슈에 대한 문제 및 안전 확보를 위한 공공·민간 전문가 집단의 논의 필요성 제기⁵⁾
 - 메타버스가 구현하는 몰입감 높은 3차원 공간에서의 다중 간의 상호작용은 원치 않는 접촉의 가능성을 증대시키며, 이는 광범위한 사이버 폭력과 개인정보 노출로 이어질 수 있음을 경고
- 현실세계에서는 불가능하지만 향후 가상융합적 공간에서 손쉽게 범죄화될 수 있는 새로운 이슈들에 대한 규제 논의 및 건강한 콘텐츠 환경 유지를 위한 인센티브의 필요성을 동시 강조

2. 미국의 메타버스 내 개인정보 활용 규제 및 사이버보안 현대화 논의

- 미국의 경우, 의회는 아직 메타버스 서비스에 대해 직접적인 언급이나 규제안을 마련하고 있지는 않지만, 최근 메타버스 공간에서의 개인정보 문제에 관심 갖기 시작⁶⁾
 - 메타버스를 구현하는 AR·VR 기술의 알고리즘이 수집할 수 있는 개인 데이터의 허용 범위에 대해 하원에서 문제를 제기
 - 미국 일부 주의 개인정보보호법의 경우, 얼굴 인식 및 지문과 같은 식별 도구가 관심을 끌면서 식별목적의 생체 정보 수집을 폭넓게 허용 중이는 기업이 당위적으로는 식별 목적을 내세움으로써 상당한 양의 데이터를 상업적으로 계속 수집·활용할 수 있는 허점을 제공

5) "How to address digital safety in the metaverse", World Economic Forum, (14 Jan 2022), <[https:// www.weforum.org/agenda/2022/01/metaverse-risks-challenges-digital-safety/](https://www.weforum.org/agenda/2022/01/metaverse-risks-challenges-digital-safety/)> (검색일: 2021.2.13.).

6) Roberto Di Pietro, Makenzie Holland, "Federal regulatory efforts could affect VR, metaverse", (06 April 2022), <[https:// modern diplomacy.eu/2022/04/06/the-metaverse-technology-privacy-and-security-risks-and-the-road-ahead/](https://modern diplomacy.eu/2022/04/06/the-metaverse-technology-privacy-and-security-risks-and-the-road-ahead/)> (검색일: 2022.3.23.).

- 메타버스의 특징인 자유롭고 열린 공간에서 표현의 자유 및 서비스의 범위와 한계를 어떻게 제한할 것인지 논의가 진행 중
- 미국 CISA 연방정부 보호실행계획(‘20.10)에서는 사이버위협 정보공유체계 개선을 통한 혁신적 사이버 보안 강화를 목표로 천명하였으며, 여기에는 메타버스를 구현하는 XR, 블록체인, 디지털 트윈이 중점분야로 반영
- 2021년 바이든행정부는 Solar Winds, MS Exchange Server 등 제어체계의 해킹사건을 계기로 사이버물리 공격에 대한 보안 증진과 연방정부 네트워크 보호를 위해 ‘국가 사이버보안 향상에 관한 행정명령(Executive Order 14028)을 발표⁷⁾

3. EU 집행위원회의 개인정보 및 디지털 거래수단 개선안 검토

- EU 집행위원회는 메타버스를 통해 ‘신상털기(doxing)’과 같이 당사자 동의 없이 개인정보를 무분별하게 노출하는 행위들이 메타버스에서 빈번하게 일어날 수 있음을 경고⁸⁾
- 또한, 메타버스에서의 효과적인 통용 수단으로 부상하고 있는 NFT 기반 거래시스템에 대한 체계적인 관리방안에도 주목한 바 있음⁹⁾
 - NFT 탈중앙금융(DeFi), NFT(대체불가토큰)을 통한 자금세탁 가능성을 막기 위한 법률 논의에 착수
 - 개인이나 법인이 직간접적으로 통제하는 탈중앙자율조직(DAO)을 EU 자금세탁·테러자금 조달 규정을 통해 규제할 필요성을 강조¹⁰⁾
 - ※ 개발자, 보유자, 운영자는 소프트웨어나 플랫폼을 출시, 이용하기 전에 자금세탁, 불량정권 지원, 테러자금 조달 등에 관한 위험평가 실시를 의무화

7) <https://www.whitehouse.gov/briefing-room/statements-releases/2021/05/12/fact-sheet-president-signs-executive-order-charting-new-course-to-improve-the-nations-cybersecurity-and-protect-federal-government-networks/>

8) “The Metaverse: Technology, Privacy and Security Risks, and the Road Ahead”, *Modern Diplomacy* (April 6, 2022), <<https://moderndiplomacy.eu/2022/04/06/the-metaverse-technology-privacy-and-security-risks-and-the-road-ahead/>> (검색일: 2022.4.10).

9) NFT는 블록체인 기술을 이용하여 디지털 자산의 소유주를 증명하는 가상의 대체불가토큰(NFT: Non Fungible Token)으로서 디지털 재화의 원본성 및 소유권을 나타내는 용도로 사용되는 진품 증명서라 할 수 있다. “메타버스 규제에 대한 이해가 필요: EU 위원이 발언” 『코인코드』, (2022.2.10), <<https://coincode.kr/archives/66927>> (검색일: 2022.4.7.).

10) <https://www.tokenpost.kr/article-107245> (검색일: 2022.9.30.).

4. 中 CICIR에서 경고한 국가안보 위협요소로서의 메타버스

- 중국 국가안전부 산하 싱크탱크인 중국현대국제관계연구원(CICIR)은 메타버스가 내포하고 있는 다양한 안보적 위험성을 경고하며 당국의 적극적인 규제와 지도를 주문¹¹⁾
 - 아직 초기 개발단계이지만, 메타버스의 기술적 특징과 개발 패턴을 볼 때, 향후 사이버안보 위협부터 기술 패권 문제에 이르기까지 잠재적인 국가안보 위협요소를 내포하고 있음을 지적
- 오픈 플랫폼 형태인 메타버스가 각국의 정치체제와 경제·사회 전반에 막대한 영향을 끼칠 수 있으며, 특히, 정치적 사상과 문화적 가치 등이 교묘하게 침투되어 안보에 중요한 위협이 될 것이라 경고
 - 특히, 메타버스가 제공하는 고도의 몰입형 경험이 ‘디지털 마약’과 같이 새로운 중독을 낳으며 현실로부터의 도피 풍조를 확산시킬 것이라 우려
- 구글, 유튜브, 페이스북 등 미국 플랫폼 기업들의 진출을 오래전부터 막아왔던 당국은 바이두, 텐센트, 바이트댄스, 넷이즈 등 자국 대기업, 스타트업들의 메타버스 사업 진출에 대해서도 경계하기 시작
- CBIRC(중국은행보험감독관리위원회)는 최근 메타버스 관련 불법 모금과 신용사기에 악용되고 있으며 특히, NFT를 악용한 다양한 활동이 중국 전역에서 이뤄지고 있다고 부연¹²⁾

5. 국내의 ‘안전하고 신뢰할 수 있는 메타버스 환경 조성’ 전략

- 국내에서는 지난 2022년 1월, 범정부 차원에서 “메타버스 신산업 선도전략”을 발표하였으며, 주요 추진전략으로 ‘안전하고 신뢰할 수 있는 메타버스 환경 조성’ 및 ‘메타버스 공동체 가치 실현’을 명시¹³⁾

11) “중국 싱크탱크 ‘메타버스, 잠재적 국가안보 위협 안아’” 『연합뉴스』, (2021.11.2.), <[https:// www.yna.co.kr/view/AKR20211102089500074](https://www.yna.co.kr/view/AKR20211102089500074)> (검색일: 2022.4.10).

12) “중국 당국 ‘메타버스 관련 4종 사기 주의’ 경고” 『연합뉴스』, (2022.2.19.). <<https://www.yna.co.kr/view/KR20220219046000074>> (검색일: 2022.4.12).

13) 관계부처합동, “메타버스 신산업 선도전략”, (2022.1.20.), pp. 47-48.

- 메타버스 생태계 참여자가 안전과 신뢰 구축을 위해 추구해야 할 자율규범으로 ‘메타버스 윤리원칙’ 수립을 추진하며, 비윤리적·불법적 행위 발생, 디지털 자산 거래 증가 등의 쟁점 해소를 위한 법제 정비 필요성 강조
 - 메타버스 서비스의 법적 성격 명확화, 아바타의 범죄 행위 처벌 실효성 확보 및 인격권 인정 여부, 거래관계 명확화 및 불공정 거래 방지 등
 - 또한 학교의 원격교육 현장에서부터, 기업 커뮤니티 가이드라인에 이르기까지 산업현장까지 포함할 수 있도록 설명
- 메타버스 환경에서 수집·활용될 수 있는 새로운 유형의 개인정보 침해 및 디지털 자산 탈취 방지를 위한 제도개선 연구 추진
 - 메타버스 내 개인정보의 범위, 메타버스 개발자 및 서비스 제공자가 이용자의 개인정보 수집·이용 시 준수해야 하는 사항 구체화 등을 포함

[그림 1] 안전하고 신뢰할 수 있는 메타버스 환경조성의 주요 내용



*출처: 관계부처합동(2022), p. 47.

III. 메타버스 공간의 확장·진화에 따른 안보위협 이슈 전망

1. 동시다발적 사이버 피해를 유발하는 ‘사이버 팬데믹’ 위협

- 디지털 가상과 물리적 현실이 연결된 메타버스 환경에서는 특정 플랫폼을 이용하여 전력망, 수처리 시설, 의료 시스템 등 사회의 필수 인프라를 타겟으로 하는 ‘사이버 팬데믹’의 발생 가능성 역시 증대
 - 사이버 팬데믹은 사물인터넷(IoT) 기반의 원격 공격을 통해 동시다발적인 바이러스 감염을 유발, 시스템 전반의 작동 이상이 나타나는 현상을 의미(WEF, 2021)¹⁴⁾
 - ※ 웹 바이러스가 대표적이며, 2017년 5월 전세계 시스템을 강타한 ‘WannaCry’(랜섬웨어와 웹 바이러스의 특징이 결합된 형태)는 빠른 전파와 파일 암호화를 동시에 진행하여 큰 피해를 유발¹⁵⁾
 - ※ 2018년 유사한 피해를 경험한 TSMC는 제조 공장을 일시 폐쇄하여 최대 40억 달러에 달하는 경제적 손실 발생한 바 있음¹⁶⁾
 - 특히, 메타버스 공간에서는 현실세계 모사나 몰입감 증대를 위해 AI 기반 소프트웨어가 다양하게 적용되며, 이들에게 부여된 자동화 학습 기능은 웹 바이러스와 유사한 공격이 전파될 수 있는 기반으로 작용
- 메타버스 플랫폼 환경은 이용자 누구나 새로운 서비스와 아이템을 개발하거나 개선할 수 있도록 공개되어 있어서 참여 과정에서 다양한 사이버공격에 대한 취약성을 내재¹⁷⁾

14) WhatIs MyIPAddress, “We’re in a Cyber Pandemic — Here’s What You Can Do About It”, <https://whatismyipaddress.com/were-in-a-cyber-pandemic-heres-what-you-can-do-about-it> (검색일: 2022.9.30.).

15) “The chronicle of WannaCry”, Enoch Root, (2022.8.23.), <<https://www.kaspersky.com/blog/wannacry-history-lessons/45234/>> (검색일: 2022.9.8.).

16) ““WannaCry” ransomware attack losses could reach \$4 billion”, CBS News, (2017.5.16.) <<https://www.cbsnews.com/news/wannacry-ransomware-attacks-wannacry-virus-losses/>> (검색일: 2022.9.8.).

17) “Trojanized dnSpy app drops malware cocktail on researchers, devs” (2022.1.8.), <<https://www.bleepingcomputer.com/news/security/trojanized-dnspey-app-drops-malware-cocktail-on-researchers-devs/>> (검색일: 2022.9.6.).

※ 개발자에 대한 피싱 공격을 통해 얻은 자격증명으로 오염된 소스 코드를 업로드하거나, 변조된 .NET 디컴파일러 dnSpy로 악성코드를 유포하려는 시도가 나타난 바 있음¹⁸⁾

- 최근 감행되고 있는 피싱 공격들은 주요 기관·기업뿐 아니라 주요 사회기반 시설에 침투하는 공격 형태로 발현되고 있으며, ‘메타워크’ 환경에서의 운영기술을 노리는 랜섬웨어, 사이버 스파이 활동 역시 증가하고 있음¹⁹⁾
 - 메타워크 애플리케이션의 이용 규모가 증가하면서, 해당 앱으로 위장한 스파이앱 형태의 공격 위험이 증대
 - 메타버스 공간에서의 사이버공격은 개인 이용자를 목표로 하는 것에 그치지 않고 서비스를 제공하거나 활용하는 기업, 공공기관, 앱 개발자 등 관련 참여 행위자 모두에 연쇄적으로 파급될 수 있음

2. ‘메타휴먼’을 활용한 딥페이크 심리전의 고도화 위험

- 최근 고도화되고 있는 하이브리드 형태의 정보심리전에서도 메타버스 기술을 악용할 가능성이 증대되고 있으며 새로운 도전을 야기²⁰⁾
 - 적성국이 메타버스를 통해 이용자들이 현실의 사회·국가 시스템을 부정적으로 인식하도록 유도하거나, 특정 인물·정당에 대한 여론전을 전개하는 형태로 현실 선거에 개입할 가능성 또한 증대
- 텍스트나 평면적 영상과 달리 실감형 경험을 제공하는 메타버스는 이용자의 과도한 몰입과 의존을 낳을 수 있으며, 중독, 현실과 가상세계의 구분 혼란, 사회적 부적응 등 다양한 사회적 병폐를 유발 가능

18) NPM(JavaScript package managers), PyPI (Python Package Index)를 노린 공격 등이 대표적이라 할 수 있음 “Two more malicious Python packages in the PyPI” (2022.8.16.) <Two more malicious Python packages in the PyPI> (검색일: 2022.9.6.).

19) “코로나19 사라져도 ‘사이버 팬데믹’은 계속된다” 『데이터넷』, (2022.1.9.), <<https://www.datanet.co.kr/news/articleView.html?idxno=154792>> (검색일: 2022.3.15.).

20) 송태은, “2022년 러시아-우크라이나 전쟁의 정보심리전: 내러티브·플랫폼·세 모으기 경쟁”, 『국제정치논총』, (2022), 제62집 3호, pp. 214-215.

- 메타버스 내 아바타인 ‘메타휴먼’에 ‘딥페이크(deep fake)’ 기술을 융합할 경우, 더욱 사실적인 거짓정보 창출이 가능
 - 실제 존재 인물과 같이 행동하는 가상공간 속의 메타휴먼에 인공지능 기술을 활용해 특정 인물의 얼굴이나 신체 부위를 합성할 경우, 인지적 왜곡 효과를 극대화시킬 수 있음
 - 딥페이크는 개발 코드가 오픈 소스여서 누구나 손쉽게 접할 수 있으며 과거 페이스플레이 앱을 통해 특정 얼굴을 다양한 영상물과 합성한 이미지가 SNS에서 인기리에 공유되는 등, 악용되기 쉬운 문제를 내포
- 만약, 딥페이크의 조작 대상이 일반인이나 연예인이 아닌 주요 정치인이나 영향력 높은 인물이 될 경우, 가상의 메타휴먼의 모습을 빌려 가짜뉴스와 고도화된 심리전 전개 가능²¹⁾
 - 국내에서도 지난 대선 기간 AI 메타휴먼을 홍보영상에 활용한 바 있으며, 사망한 극단 주의자들의 모습이 메타휴먼으로 부활할 경우, 초국적 테러리스트들의 결집과 대항을 주문할 가능성
 - 특히, 메타휴먼의 악용은 사회 불안을 야기시키는 ‘인포데믹스(거짓정보의 광범위한 사회적 확산)’의 부작용을 더욱 증대시킬 수 있음
- 딥페이크 영상은 SNS 뿐 아니라 방송국 등을 해킹해서 송출할 경우, 사회적 파장은 더욱 커질 수 있으며, 실제 러시아 침공 당시 뉴스채널인 ‘우크라이나24’가 가장 먼저 해킹의 표적이 되었음
 - 러시아 침공 이후 해커들은 우크라이나의 고위 군 지도자들과 정치인들의 페이스북 계정에 침입해, 항복을 알리는 허위 메시지를 게시
 - ※ 젤렌스키 우크라이나 대통령이 러시아에 항복을 선언하는 모습과 푸틴 대통령이 평화를 선언하는 모습 담은 딥페이크 영상이 유포된 바 있음²²⁾

21) 송태은(2022), p. 215.

22) BBC News Korea, “러시아-우크라이나 전쟁에 사용된 대통령 딥페이크 영상”, (2022.3.20.), <<https://www.bbc.com/korean/international-60776475>> (검색일: 2022.9.6.).

3. 디지털 재화의 거래 취약성을 악용한 대규모 가상자산의 탈취

- NFT가 메타버스 공간의 용이한 주거래 수단으로 부상하면서, 음반, 작품, 금융 서비스 등 디지털 재화의 거래량이 급증함에 따라 거래 시스템의 노출 빈도 및 악용 가능성도 증가 전망²³⁾
 - 특히, 가상화폐 금융자산은 가격 변동성이 높으며 개발자가 NFT 발행을 위한 프로젝트성 자금 공개모집 직후 갑자기 사이트를 폐쇄하고 자취를 감추는 등 신종 사기의 수법이 고도화 중
 - ※ 블록체인 데이터 기업 체이널리시스에 따르면, 최근 가상화폐로 인한 사기, 탈취 피해액은 2020년 43억 달러에서 2021년 77억 달러로 폭증²⁴⁾
- 메타버스가 탈중앙적 특징을 가진 가상화폐의 거래 방식을 악용하는 이들의 불법자금 유통 경로로 변질될 위험
 - 국가와 중앙은행이 통제·관리하는 기존의 금융시스템과 달리 가상화폐를 거래방식으로 즐겨쓰는 메타버스에서는 자금의 추적·관리가 어려워 정부 규제 및 관리의 사각지대에 놓일 수 있음
- 가상 자산의 복제는 기술적으로 어려워 사용자와 거래소를 해킹해 가상자산을 탈취하는 방법이 활용되고 있음
 - 피싱 공격이나 악성코드 감염으로 로그인 자격 증명을 확보한 후, 소유권을 이전하여 시스템에 보관된 가상 자산을 훔치는 방식으로 발생
 - ※ '22년 2월 3일, 예치금액이 20억 달러(약 2조 4,000억원)에 달하는 국내 최대 규모 디파이(Defi, 탈중앙화 금융) 서비스 '클레이스왑(KLAYswap)'에서 22억원의 가상 자산이 탈취되는 해킹 사건이 발생²⁵⁾

23) 머니투데이(2021.10.21.), 2020년 한국저작권보호원에 따르면무단 복제 후 플랫폼을 통해 유통된 온라인 불법 복제물은 약 87만건에 달하였다. “콘텐츠 불법유통 막아달라”...방송·영화사, 통신3사에 요청 <<https://news.mt.co.kr/mtview.php?no=2021102111393544863>> (검색일: 2022.1.9.).

24) 매일경제(2022.3.31.), “NFT ② 거품인가 미래인가 | 국내서도 먹튀 사기 사례 잇달아”, <<https://www.mk.co.kr/news/culture/view/2022/03/291997/>> (검색일: 2022.4.10.).

25) 한국경제(2022.2.11.), “범죄온상 된 디파이...털린 코인만 2조원 넘어”, <<https://www.hankyung.com/economy/article/2022021180861>> (검색일: 2022.3.29.).

- ※ OpenSea 사용자를 피싱 공격한 후, 소유권을 이전하도록 유도하여 170만 달러어치의 NFT가 도난당하였으며,²⁶⁾ NFT 등록 플랫폼 Premint 웹사이트를 해킹해 가짜 팝업을 띄운 뒤, 40만 달러의 NFT를 탈취한 사례 발생²⁷⁾
- ※ 2022년 호라이즌브릿지에서는 1억 달러 규모 암호화폐가 탈취 되었으며, 해커는 이를 담보로 스테이블 코인을 구입해 환전²⁸⁾

4. 비대면 소통방식을 활용한 급진주의 테러세력 지원 및 공격 조장

- VR·AR 등 메타버스 기반기술 및 지능화 기술은 잠재적으로 테러집단을 양성하거나 공격행위를 조장하는데 손쉽게 악용될 수 있음²⁹⁾
 - 메타버스의 비대면 소통 환경은 더욱 은밀한 형태로 잠재적 테러리스트들을 모집하기 용이하며 심리전, 작전예의 영향 등을 미칠 수 있음
 - 또한 NFT, 암호화폐, 블록체인 시스템을 통해 비밀리에 테러 비용을 지원하거나 자금세탁의 도구로 활용됨
 - ※ 현재 전쟁중인 러시아와 우크라이나는 국제사회로부터 기부 받은 NFT를 사이버 상에 판매, 한 달만에 6500만 달러를 확보하는 등, 오늘날 디지털 가상재화는 전쟁자금으로서의 기능까지 수행하고 있음³⁰⁾

26) 300+ NFTs Stolen, \$400K in Ethereum Taken In Premint Hack (2022.07.19.) <<https://decrypt.co/105385/300-nfts-stolen-400k-in-ethereum-taken-in-premint-hack>>

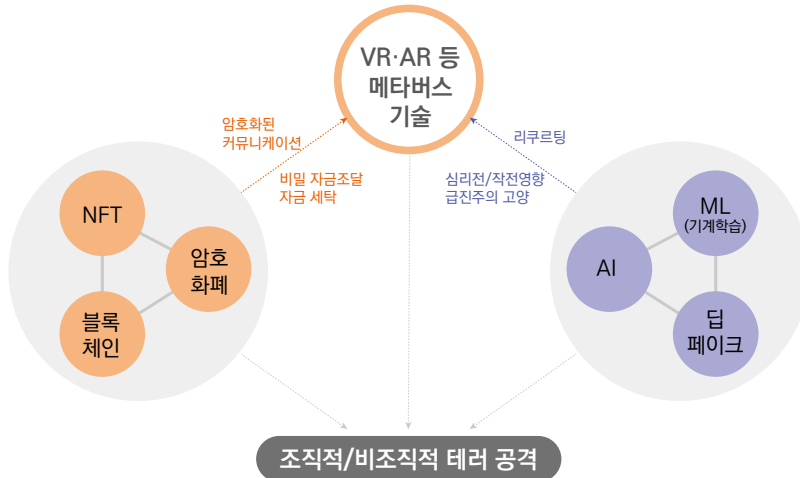
27) “‘지루한 원숭이도 털렸다’...NFT 발행 지원 플랫폼 ‘프리민트’ 해킹 ” (2022.7.17.) <<https://www.news1.kr/articles/?4745202>> (검색일: 2022.3.22.).

28) VOA, “북한 해킹조직, 미국 블록체인 회사에서 1억 달러 규모 암호화폐 탈취” (2022.7.1.) <<https://www.voakorea.com/a/6640892.html>> (검색일: 2022. 7.28).

29) World Summit on Counter-Terrorism (검색일: 2022.9.14.).

30) Cameron Thompson, “Ukraine Launches ‘NFT Museum’ to Raise Funds and Remember.” Coindesk(Mar 26, 2022). <https://www.coindesk.com/tech/2022/03/25/ukraine-launches-nft-museum-to-raise-funds-and-remember/> (검색일: 2022.10.2).

[그림 2] 잠재적 테러세력의 양성·지원 도구로 악용되는 메타버스 기술 메커니즘



* 출처: World Summit on Counter-Terrorism(2022.9.14.) 토대로 재정리

- 또한, AR·VR에서의 자극은 다른 디지털 세계의 경험에서보다 훨씬 강력한 영향을 미치며 배타적 집단에 대한 폭력을 조장할 가능성
 - 실제로 최근 “디지털 중독 문제”가 부상하는 가운데, 특히, 메타버스 가상융합형 콘텐츠가 이 같은 현상의 심화와 상관관계가 있다는 연구결과등이 보고된 바 있음
- 스마트폰 제조사 HTC와 홍콩중문대학의 연구결과에 따르면, VR게임은 일반 컴퓨터 게임보다 44% 높은 중독현상과 20% 높은 이용자의 흥분지수를 유발
 - 메타버스 플랫폼에서 표출되는 아바타 간의 폭력적 다툼, 노골적인 차별과 학대, 집단 간 혐오 현상들은 향후 사이버 폭력의 극단적 진화 양상 및 사회문제의 가능성을 암시
 - 최근 이주민에 대한 극단적 혐오, 인종차별, 온라인 학대 등의 사이버 폭력이 로블록스, 페이스북 등 다수의 플랫폼에서 행해졌으며, 피해 집단은 이로 인한 정신적 고통과 사회적 소외감을 호소³¹⁾

31) “How to address digital safety in the metaverse”, World Economic Forum, (14 Jan 2022), <<https://www.weforum.org/agenda/2022/01/metaverse-risks-challenges-digital-safety/>> (검색일: 2022.2.13.).

5. '디지털트윈' 해킹으로 인한 제어 인프라의 오작동 위험

- 메타버스 기술의 발전으로 그 동안 개념적으로만 논의되었던 '디지털 트윈' 기술을 광범위한 산업·서비스 부문에 적용할 수 있게 됨

※ Digital Twin은 위 현실세계의 물리적 자산이나 객체, 프로세스 등을 동일하게 가상에서 구현한 디지털 복제(Modeling)를 의미하며, 모양과 상태, 행동까지 그대로 반영한 것

〈참고〉 국내의 메타버스 기반 디지털 트윈의 산업·공공 부문 적용 현황

적용 분야	사업/추진 주체	서비스 내용
제조	한국전자기술연구원 포항과학산업연구원 공동	포항과학산업연구원 내 포스코케미칼 이차전지 소재 파일럿 제조 공장에서 '디지털 트윈 기반 실감기술(XR)' 도입
	GS칼텍스	디지털 트윈 관제센터 구축을계획하고 사이버 공간에서 여수 정유 공장 내 관련 30만개 설비 통합 모니터링, 3D 공간에서 시뮬레이션 교육·훈련 등을 추진
재난안전 건설토목	국토부, 과기정통부, 행안부, 산자부 합동	'디지털트윈 기반 지하공동구 화재·재난지원 통합플랫폼 기술개발' 추진
스마트 시티	서울시	도시전역을 최신 3D 공간정보(디지털 트윈)으로 구축하는 '버추얼 서울' 기반 도시계획(일조권, 건축물 배치, 교통량), 기후환경(대기질, 도시열섬), 재난안전(홍수, 산사태, 소방) 서비스 제공
농림수산 항만	LG유플러스	5G망 기반 트랙터 원격 제어 및 무인 경작과 디지털 트윈 기술을 이용한 트랙터 원격진단 서비스를 추진
에너지	한국전력	클라우드 가상화 기술기반 공통 플랫폼(HUB-PoP)개발 및 관련 차세대 배전 지능화 플랫폼, 지능형 디지털 발전소 개발을 추진 중
의료	과기정통부·국방부	국군간호사관생도 등 의료진 대상으로 실제 재현이 어려운 중증 외상 처치훈련 시스템 구축개발(~'22)
	과기정통부	환자데이터 기반 메디컬 트윈 구현 및 XR 가상화를 통해 진단·예측-교육-수술 솔루션 개발실증사업 추진('22~)
	메디컬아이피 (국내 의료 SW업체)	AI에 기반 3D모델링 기술로 인체 내부 정보를 모델링한 의료용 3D프린팅 제품 '아나텔(ANATDEL)' 제작

*출처: KISA Insight(2021), 이승민(2022)를 토대로 재구성.

- 사이버-물리시스템의 융합공간으로서 메타버스가 갖는 특징을 고려할 때, 가상세계에서의 해킹은 현실세계에서의 물리적 피해를 가할 수 있는 중대한 위협으로 전환될 수 있음
 - 디지털트윈 구축을 위해 수집되는 데이터 중 시설·제어·인프라 등 중요 정보의 유출과 위변조 시, 오작동 및 센서 조작 사고 발생 가능
 - 메타버스 기반 인프라 관련 시스템에 대한 공격은 디지털 제어를 통한 대규모 물리적 피해의 발생 가능성을 확인한 사례
 - ※ 이란 부셰르 원전을 공격해 원전 운영에 영향을 끼친 Stuxnet은 국가 주요 산업 시설에 장애를 일으키고자 제작된 최초의 악성코드로 특정 국가의 지원 아래 제작된 것으로 추정됨³²⁾
 - ※ 전력망을 공격한 최초의 악성코드인 Industroyer는 2016년 12월 우크라이나 일부 지역에 정전을 일으켰으며,³³⁾ 2022년에도 러시아 해킹그룹 Sandworm은 Industroyer 2를 이용해 우크라이나 공격 시도³⁴⁾
- 스피어피싱(Spearfishing) 공격과 유사한 방식으로 공격자가 디지털트윈 내에서 인프라 모니터링·제어를 담당하는 작업자를 속여 제어 인프라의 접근 권한을 탈취할 가능성
 - 현실세계와는 달리 메타버스 내에서는 이용자가 자신이 위치한 장소나 환경의 진위 여부를 판단하기 어려운 만큼, 공격자가 특정인을 대상으로 꾸며놓은 메타버스 작업환경 내에서 시스템 접근·조작 관련 중요 정보를 노출할 우려 존재

6. 생체정보 등 민감정보 수집을 통한 집단 프로파일링의 악용 가능성

- 메타버스에서는 이용자들의 모든 행동 정보가 관찰·기록될 수 있으며, 이러한 데이터가 가공·유통되어 악의적 주체에게 넘어갈 경우에는 이용자를 통제하는 수단으로 활용될 가능성이 존재
 - 3D 가상입체 공간인 메타버스에 축적된 이용자 및 아바타의 활동 기록은 기존의 텍스트, 영상 정보와 비교불가한 방대하고 입체적인 데이터 세계의 창출을 의미

32) 안랩, (2010.10.19.), “악성코드의 새로운 패러다임, Stuxnet”, https://www.ahnlab.com/kr/site/securityinfo/secuNews/secuNewsView.do?menu_dist=2&seq=16852 (검색일: 2022. 9. 1).

33) Reuters, Ukraine’s power outage was a cyber attack: Ukrenergo”, (2017.1.18.), <<https://www.reuters.com/article/us-ukraine-cyber-attack-energy-idUSKBN1521BA>> (검색일: 2022. 9. 1).

34) “Russia’s Sandworm Hackers Attempted a Third Blackout in Ukraine”, Wired, (2022.4.12.), <<https://www.wired.com/story/sandworm-russia-ukraine-blackout-gru/>> (검색일: 2022. 8. 11).

- 실제 환경에서도 CCTV, IoT 기기 등을 통해 사람들의 행동과 상태 정보가 수집될 수 있으나 개개인이 이를 회피할 방법이 존재하는 것과는 달리, 메타버스에서는 이용자의 몸짓, 시선 등 사소한 개인적 활동과 생체 정보까지도 해킹의 대상이 수 있음
 - ※ 메타(舊 페이스북)는 메타버스 이용자들이 착용하는 장치(HMD)를 통해 이용자의 표정을 감지해 이를 바탕으로 콘텐츠를 맞춤 제공하는 기능, 이용자의 자세와 같은 신체 데이터를 수집하는 기능 등에 대한 특허를 확보, 상업적 이용에 광범위한 활용 가능성을 암시³⁵⁾
- 메타버스 내 아바타의 행동을 면밀히 분석하는 것만으로도 해당 아바타를 조작하는 사람의 성별, 나이, 직업, 성향 등 정확한 프로필을 유추해 낼 수 있으며, 이는 현실세계나 메타버스 내의 개인과 집단에 대한 공격에 활용될 수 있음
- 특정인과 관련된 데이터를 다양한 방법으로 수집하여 개인을 넘어 집단 특성 정보를 생성하는 ‘프로파일링(Profiling)’의 악용 가능성 존재
 - ※ 온라인 광고(고객의 성별, 나이 등을 추정하여 결과에 부합하는 맞춤형 광고 송출), 콘텐츠 추천(이용자의 검색기록을 분석을 통해 검색 의도를 추정하여 추천 목록 자동 표출), 금융거래 감시(이용자의 금융·비금융 활동 정보를 분석하여 부정거래 행위 사전 차단) 등에 AI 기반의 프로파일링이 활발히 활용되고 있음

IV. 시사점과 대응 방안

1. 신종 사이버 위협으로서 메타버스 리스크에 대한 거시적 이해 필요

- 각국은 현재까지 메타버스가 가진 잠재적 리스크보다는 새로운 시장창출 및 산업생태계 육성 측면을 보다 주목해왔음
 - 그러나 메타버스 산업의 급속한 성장은 다양한 위험요소를 내포하고 있으며 ‘가상융합 공간’에 부합하는 법·제도의 시급한 보완을 요구

35) <https://www.ft.com/content/76d40aac-034e-4e0b-95eb-c5d34146f647> (검색일: 2022. 9. 3).

- 또한, 메타버스 패러다임이 초래하는 광범위한 국가안보적 위협요소에 대한 대응과 논의는 주로 현재적·미시적 관점에 머물러 있음
- 메타버스를 단순한 기술 발전이 아닌, 사회 전반의 디지털 고도화 과정으로 이해하고, 국가 안보적 리스크에 대한 진단과 평가 이 같은 거시적 환경변화의 맥락에서 분석할 필요
 - 향후 개인이나 해커집단이 아닌, 국가가 전면에서 메타버스 기반 공격과 방어 기술을 전력화한다면, 현재의 사이버전보다 더욱 진화된 형태의 하이브리드전 양상도 등장 가능

2. 가상과 현실의 '위협의 동기화'에 대비한 거버넌스 체계 수립 필요

- 향후 메타버스 윤리 가이드라인 등 쟁점사항을 실효적인 정책으로 구체화할 수 있도록 민관 협력체계 윤리제도분과 운영 활성화 필요
 - 민간기업 '메타'는 자사의 호라이즌 월드에서 사용자 보호를 위한 개인 경계(Personal Boundary)를 도입 중설행
- 위협의 온오프라인 구분 경계가 모호해지는 환경에서 메타버스를 활용한 통합적 안보 리스크를 예방하기 위한 사이버-물리체계의 연결 취약점 진단 및 정보보호체계 개선 노력 필요
 - 가상융합 인프라 및 시스템, 네트워크, 데이터 등 메타버스 서비스를 이루는 생태계 각 분야의 보안 내재화 및 표준 가이드라인 마련 등
- 특히 가상과 현실의 위협이 동시에 발생하는 '위협의 동기화' 환경이 제공하는 메타버스 안보 위협에 대한 거버넌스 조정 및 대응체계 필요
 - 평시의 사이버 위기고조에서 전시의 물리적 제어시스템의 공격에 이르기까지 공간의 경계를 초월한 '위협의 동기화' 상황에 대한 다양한 시나리오 수립 및 대응 매뉴얼 구축이 요구됨
 - 또한, 공공부문, 방송통신, 과학기술, 금융, 국방 등 메타버스 리스크가 포괄하는 광범위한 위협들에 대해 실무 기관별 실시간 분석 및 정보 공유가 가능하도록 범정부 협력체계 강화 필요

3. 신종 디지털트윈 공격 예방을 위한 ‘능동적 억지’ 전략 수립

- 메타버스의 디지털트윈을 통해 통째로 사이버 공격의 목표물에 대한 실시간 정보를 획득하고 이를 전력에 제공한다면, 재래식 무기의 효과 또한 극대화될 가능성
 - 현재 ‘디지털트윈’ 기술은 산업·공공 정책 부문에 활용되고 있으나, AI, 5G 클라우드와 접목된 군사무기체계로 개발되어 원격 목표물을 노린 사이버 공격기술로 전용된다면 치명적 위협이 될 수 있음
 - 이를 위해, 국가 핵심 제어인프라 분야에서는 보다 엄격한 ‘제로 트러스트’ 개념에 기반한 검증모델 도입과 메타버스 위협에 선제적으로 대응하는 ‘능동적 억지 전략’ 도입 필요
 - ※ Zero Trust Architecture: 위협이 기존 네트워크의 내부와 외부 모두에 존재한다는 인식에 기반한 보안 모델, 일련의 시스템 설계 원칙, 조정된 사이버 보안 및 시스템 관리 전략을 의미하며, 최소한의 액세스만 허용하고 변칙적이나 악의적인 활동을 모니터링하는 개념
 - ※ 美바이든 행정부는 사이버보안 현대화를 위해 △제로 트러스트 아키텍처(Zero Trust Architecture) △클라우드 보안 가속화 △다중 요소 인증 및 암호화 채택 등을 포함한 바 있음

4. 메타버스 데이터·금융거래에 대한 국가의 관리기능 강화

- 메타버스에 축적된 기업·집단·국가 단위의 방대한 활동 데이터는 다양한 정보·심리전과 선동의 도구로 활용될 수 있어 ‘데이터 지리적경계(geofencing)’와 같은 메타버스 데이터 거래에 적용되는 가이드라인 마련 필요
 - 특히, 데이터가 국가 단위의 안보위협국으로 유입되는 것을 방지하기 위해, 국내 이용자나 국산 메타버스 서비스에서 발생한 데이터는 가공 여부를 막론하고 해외 반출을 모니터링할 필요
- 국내 이용자들이 안보 위협국이 직접 운영하거나 운영을 지원하는 메타버스를 이용하는 것을 억제하기 위한 정책적 수단을 확보할 필요

- 국가안보에 위협이 될 수 있는 국가의 기업이 국내 시장에 진입하는 것은 국가안보 차원에서 심각하게 고려되어야 하며, 국내 기업에 대한 지분 참여나 인수·합병도 최소한으로 허용하여야 할 것
- 디지털 자산 거래의 경우, 신뢰할 수 있는 제3기관을 통해 NFT로 거래되는 디지털 자산의 진본 여부를 검증하는 제도 도입을 검토하고 중·장기적으로 전담기관 마련을 모색할 필요
- 당사자 간 원활한 거래 뿐만 아니라 보안성이 증진된 환경 구축이 전제되어야 하며, 실질적인 관리 역할을 수행할 NFT 크리에이터 전문가 육성도 필요

참고문헌

- 과학기술정보통신부. 2021. “'21년 사이버위협 분석 및 '22년 전망 분석”, (2021.12.24.).
- 관계부처합동. 2022. “메타버스 신산업 선도전략”, (2022.1.20.).
- 김상균·신병호, 2021. 『메타버스: 새로운 기회 디지털 지구, 경제와 투자의 기준이 바뀐다』, 서울: 베가북스.
- 송태은. 2022. “2022년 러시아-우크라이나 전쟁의 정보심리전: 내러티브·플랫폼·세 모으기 경쟁”, 『국제정치논총』, 제62집 3호. pp. 213-255.
- 이승민. 2022. 『메타버스와 법: 그 물음표(?)와 느낌표(!)』, 서울: 박영사.
- KISA. 2022. “메타버스와 NFT, 사이버보안 위협 전망 및 분석”, 『KISA Insight』, Vol. 4.
- Smart, J.M., Cascio, J. and Paffendorf, J.(2010), “Metaverse Roadmap Overview, 2007”. Accelerated Studies Foundation. Retrieved.
- World Summit on Counter-Terrorism(2022.9.14.).
- 데이티넷. “코로나19 사라져도 ‘사이버 팬데믹’은 계속된다” (2022.1.9.), <<https://www.datanet.co.kr/news/articleView.html?idxno=154792>> (검색일: 2022.3.15.).
- 매일경제(2022.3.31.), “NFT ② 거품인가 미래인가 | 국내서도 먹튀 사기 사례 잇달아”, <<https://www.mk.co.kr/news/culture/view/2022/03/291997/>> (검색일: 2022.4.10.).
- 머니투데이(2021.10.21.), 2020년 한국저작권보호원에 따르면 무단 복제 후 플랫폼을 통해 유통된 온라인 불법 복제물은 약 87만건에 달하였다. “콘텐츠 불법유통 막아달라’…방송·영화사, 통신3사에 요청” <<https://news.mt.co.kr/mtview.php?no=2021102111393544863>> (검색일: 2022.1.9.).
- 안랩, (2010.10.19.), “악성코드의 새로운 패러다임, Stuxnet”, https://www.ahnlab.com/kr/site/securityinfo/secunews/secuNewsView.do?menu_dist=2&seq=16852 (검색일: 2022. 9. 1).
- 연합뉴스. 2022. “중국 당국 ‘메타버스 관련 4종 사기 주의’ 경고” 『연합뉴스』, (2022.2.19.). <<https://www.yna.co.kr/view/KR20220219046000074>> (검색일: 2022.4.12.).
- 코인코드. 2022. “‘메타버스 규제에 대한 이해가 필요’ EU 위원이 발언” (2022.2.10), <<https://coincode.kr/archives/66927>> (검색일: 2022.4.7.).
- 한국경제(2022.2.11.), “범죄온상 된 디파이…털린 코인만 2조원 넘어”, <<https://www.hankyung.com/economy/article/2022021180861>> (검색일: 2022.3.29.).

- Abrams, Lawrence. 2022. "Trojanized dnSpy app drops malware cocktail on researchers, devs" (2022.1.8.), <<https://www.bleepingcomputer.com/news/security/trojanized-dnsPY-app-drops-malware-cocktail-on-researchers-devs/>> (검색일: 2022.9.6.).
- BBC News Korea, "러시아-우크라이나 전쟁에 사용된 대통령 뱃지 영상", (2022.3.20.), <<https://www.bbc.com/korean/international-60776475>> (검색일: 2022.9.6.).
- Cameron Thompson, "Ukraine Launches 'NFT Museum' to Raise Funds and Remember."
- CBS News. 2022. "'WannaCry' ransomware attack losses could reach \$4 billion", (2017.5.16.) <<https://www.cbsnews.com/news/wannacry-ransomware-attacks-wannacry-virus-losses/>> (검색일: 2022.9.8.).
- Coindesk(Mar 26, 2022). <https://www.coindesk.com/tech/2022/03/25/ukraine-launches-nft-museum-to-raise-funds-and-remember/> (검색일: 2022.10.2.).
- Enoch Root, 2022. "The chronicle of WannaCry", (2022.8.23.), <<https://www.kaspersky.com/blog/wannacry-history-lessons/45234/>> (검색일: 2022.9.8.).
- Financial Times. <https://www.ft.com/content/76d40aac-034e-4e0b-95eb-c5d34146f647> (검색일: 2022.9.3.).
- KT Enterprise (2022.1.28.). "메타노믹스 시대의 세 가지 과제" <https://post.naver.com/viewer/postView.naver?volumeNo=33252572&memberNo=6457418&vType=VERTICAL> (검색일: 2022. 5. 5.).
- Modern Diplomacy. 2022. "The Metaverse: Technology, Privacy and Security Risks, and the Road Ahead", (April 6, 2022), <<https://moderndiplomacy.eu/2022/04/06/the-metaverse-technology-privacy-and-security-risks-and-the-road-ahead/>> (검색일: 2022.4.10.).
- News1. 2022. "'지루한 원숭이도 털렸다'...NFT 발행 지원 플랫폼 '프리미트' 해킹" (2022.7.17.) <<https://www.news1.kr/articles/?4745202>> (검색일: 2022.3.22.).
- NPM(JavaScript package managers), PyPI (Python Package Index)를 노린 공격 등이 대표적이라 할 수 있음 "Two more malicious Python packages in the PyPI" (2022.8.16.) <Two more malicious Python packages in the PyPI> (검색일: 2022.9.6.).
- Pietro, Roberto Di. 2022. Makenzie Holland, "Federal regulatory efforts could affect VR, metaverse", (06 April 2022), <<https://moderndiplomacy.eu/2022/04/06/the-metaverse-technology-privacy-and-security-risks-and-the-road-ahead/>> (검색일: 2022.3.23.).
- Reuters, "Ukraine's power outage was a cyber attack: Ukrenergo", (2017.1.18.), <<https://www.reuters.com/article/us-ukraine-cyber-attack-energy-idUSKBN1521BA>> (검색일: 2022. 9. 1)

- The White House. 2022. <https://www.whitehouse.gov/briefing-room/statements-releases/2021/05/12/fact-sheet-president-signs-executive-order-charting-new-course-to-improve-the-nations-cybersecurity-and-protect-federal-government-networks/> (검색일: 2022. 9.21.).
- Token Post. 2022. <https://www.tokenpost.kr/article-107245> (검색일: 2022.9.30.).
- VOA, “북한 해킹조직, 미국 블록체인 회사에서 1억 달러 규모 암호화폐 탈취” (2022.7.1.) <<https://www.voakorea.com/a/6640892.html>> (검색일: 2022. 7.28).
- WhatIs MyIPAddress, “We’re in a Cyber Pandemic – Here’s What You Can Do About It”, <https://whatismyipaddress.com/were-in-a-cyber-pandemic-heres-what-you-can-do-about-it> (검색일: 2022.9.30.).
- WEF. 2022. “How to address digital safety in the metaverse”, World Economic Forum, (14 Jan 2022), <<https://www.weforum.org/agenda/2022/01/metaverse-risks-challenges-digital-safety/>> (검색일: 2022.2.13.).
- Wired. 2022. “Russia’s Sandworm Hackers Attempted a Third Blackout in Ukraine”, (2022.4.12.), <<https://www.wired.com/story/sandworm-russia-ukraine-blackout-gru/>> (검색일: 2022. 8. 11).

Abstract

Metaverse risk outlook as a national security issue

Junghyun Yoon

(Institute for National Security Strategy)

Today, 'Metaverse' is emerging based on the non-face-to-face trend triggered by COVID-19. However, the expansion of the metaverse activity area is increasing the vulnerability to cyber threats and expanding the scope of the threats that transcend the boundaries between virtual and real. In addition, the approach and institutional preparation from the national security perspective are still insufficient for quantitative and qualitative changes in cyber threats based on metaverse. Therefore, this study aims to predict the wide range of national security threats caused by the metaverse paradigm and propose an approach direction. It is required to respond urgently at the national level to new forms of metaverse risks such as cyber pandemic, deepfake, deprivation of virtual assets, support for terrorists, digital twin-based hacking, and sensitivity information profiling. As a new cyber threat, macroscopic understanding of metaverse risks, establishment of governance system in preparation for 'synchronization of threats', establishment of 'active deterrence' strategy to prevent new digital twin attacks, and strengthening of the state's management function for metaverse data and financial transactions are representative.

Keywords: metaverse, virtual shared space, cyber pandemic, digital twin, NFT

INSS

전략보고

October 2022. No.184

국가안보전략연구원

📍 06295 서울시 강남구 언주로 120 인스토피아 빌딩
☎ 02-6191-1000 📠 02-6191-1111 🌐 www.inss.re.kr